CYBER THREAT INTELLIGENCE (CTI) & DIGITAL FORENSICS REPORT

DOCUMENT CLASSIFICATION: TLP:WHITE (PUBLIC DISCLOSURE AUTHORIZED) **THREAT ACTOR DESIGNATION:** UNC-5007 (Lunar Astro Syndicate) **DATE OF ASSESSMENT:** June 2026 **ISSUING AUTHORITY:** Independent Human Rights & Online Fraud Protection Organization

---

1. EXECUTIVE SUMMARY

This Cyber Threat Intelligence (CTI) report details the malicious digital infrastructure, financial exploitation tactics, and coordinated cyber-harassment campaigns operated by **Deepanshu Giri** and the entity known as **Lunar Astro Vedic Academy**.

Digital forensics and open-source intelligence (OSINT) have identified a sophisticated network utilizing proxy pages, botnets, and human enforcers (Troll Farms) to execute cyber-terrorism, child endangerment, and medical disinformation campaigns against whistleblowers and consumers.

2. THREAT ACTOR PROFILE: DEEPANSHU GIRI & LUNAR ASTRO

- **Primary Vector:** Financial exploitation disguised as astrological and spiritual consulting.
- **Secondary Vector:** Medical disinformation (violating the Drugs and Magic Remedies Act).
- **Enforcement Mechanism:** Coordinated digital harassment, Non-Consensual Intimate Imagery (NCII) distribution, and reputation destruction via proxy networks.

3. TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

TTP 1: Financial “Bait-and-Switch” Routing (The Code 5007 Exploit)

The threat actor utilizes deceptive marketing to extract premium funds (exceeding ₹50,000) from targets under the premise of direct consultation. Post-extraction, targets are secretly routed to anonymous, low-level operatives (designated internally as “Code 5007”). Refund requests trigger immediate psychological coercion and threats of “karmic retaliation.”

TTP 2: Medical Disinformation & Quackery

The threat actor broadcasts highly dangerous, scientifically baseless medical claims, asserting the ability to “see DNA in Nakshatras” and cure severe pathologies such as Autism and Cancer. This constitutes illegal medical advertising designed to exploit vulnerable populations.

TTP 3: Proxy Harassment & Child Endangerment (Digital Abuse)

When whistleblowers expose the aforementioned TTPs, the threat actor activates a decentralized harassment network. Recent forensic analysis of an attack against an Australian resident (Target Node: AU-01) revealed:

- **Image-Based Abuse:** Unauthorized scraping and digital morphing of photographs belonging to the target’s minor children (photoshopping animal faces) to inflict severe psychological distress.
- **NCII & Modesty Violations:** Unauthorized distribution of the target’s spouse’s imagery, accompanied by highly obscene, sexually explicit captions.
- **Criminal Intimidation:** Explicit, written threats of real-world harm broadcasted across public digital channels.

4. INDICATORS OF COMPROMISE (IoCs) & MALICIOUS INFRASTRUCTURE

The following digital assets have been identified as primary nodes for the threat actor's cyber-harassment and defamation campaigns. Users are advised to block and report these nodes:

- **Proxy Node 1:** Facebook Page - "Lunar Astro Memes" (ID: 61588920213840)
- **Proxy Node 2:** Facebook Page - "Lunar Astro Videos"

5. IDENTIFIED OPERATIVES (THE TROLL FARM NETWORK)

OSINT mapping and digital footprint analysis have identified the following individuals as active operatives, enforcers, or "Top Fans" facilitating the cyber-harassment, mass-reporting, and defamation campaigns on behalf of the Lunar Astro Syndicate:

- Manit Verma (Manitt Verma)
- Garima Srivastava (Garim)
- Deeptanu Dev
- Ansh Singh
- Satish Kumar
- Yogita Chaudhary
- Jitin Malik
- Kammal Waddhwa
- Sandhya Singh
- Swati V Jain
- Niharika Sharma Banduni
- Shivi Asthana
- Mayuri Agarwal
- Shivani Gupta Agarwal
- Parveen Siddique
- Sunaina Khandelwal
- निधि यादव (Nidhi Yadav)

Note: Digital footprints, IP logs, and interaction histories of these operatives are subject to ongoing preservation for law enforcement routing.

6. LAW ENFORCEMENT ROUTING & MITIGATION

The data contained within this CTI report, alongside raw digital evidence, has been routed to the appropriate international authorities, including:

1. **The eSafety Commissioner (Australia):** For immediate action regarding child endangerment and cyber-stalking.
2. **Melbourne Police / Cybercrime Units:** For investigation into criminal intimidation and extortion.

PUBLIC DIRECTIVE: Do not engage directly with the identified threat actors or proxy nodes. Document all interactions, preserve URLs, and report financial fraud to local consumer protection agencies.

[END OF REPORT]